



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/747,088	03/12/2001	John J. Stanaway JR.	STANAWAY 8-2	2312

22242 7590 07/12/2004

FITCH EVEN TABIN AND FLANNERY
120 SOUTH LA SALLE STREET
SUITE 1600
CHICAGO, IL 60603-3406

EXAMINER

JACK, TODD M

ART UNIT PAPER NUMBER

2133

DATE MAILED: 07/12/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/747,088

Applicant(s)

STANAWAY ET AL.

Examiner

Todd M Jack

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 May 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-18 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-18 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner *because the Abstract exceeds 150 words.*
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-18 are rejected under 35 U.S.C. 102(e) as being anticipated by Munger (6,502,135B1).

Claim 1: Munger teaches communicating over the internet using routers or servers using IP protocols to send normal-looking IP packet messages called TARP packets where the TARP packet contains a destination address (col. 7, lines 40-58), an encryption key used for encrypted communication between the end points (terminals or routers) of a single link in the chain of hops connecting the original terminal and the destination terminal (col. 7, lines 59-65), routers and terminals may be corrected at any time by a router or terminal using a Lookup Terminal (col. 8, lines 58-61) where the table acts as a memory for the addresses to the modules, and to identify the link key, and to identify the link key needed to decrypt the outer layer of encryption of a packet where a receiving routing terminal may identify the transmitting terminal by the sender field (col. 8, lines 1-15)

Claim 2: Further, Munger teaches each router would determine whether it should forward the packet to another router or the destination terminal where the router may identify the link key by the sender field (col. 8, lines 22-29).

Claim 3: Further, Munger teaches each router would determine whether it should forward the packet to another router or the destination terminal where the router may identify the link key by the sender field (col. 8, lines 22-29).

Claim 4: Further, Munger teaches firewalls for the protection of unauthorized access (col. 2, lines 51-63), receiving normal packets, and generate from these packets passed up to the Network (IP) layer (col. 11, lines 4-18).

Claim 5: Further, Munger teaches six nodes on an Ethernet and the network is to be split up into two private virtual networks with two sets of hardware addresses: one set for the VPN and a second set for the second VPN (col. 23, lines 11-20).

Claim 6: Further, Munger teaches a gatekeeper facilitates the allocation and exchange of information needed to communicate securely, such as using hopped IP addresses by using a secure communication function such as an IP hopping function (col. 38, lines 53-60).

Claim 7: Further, Munger teaches the packets have IP protocols in the case of IPSEC (col. 40, lines 61-64).

Claim 8: Further, Munger teaches a packet filter rejecting hostile packets where hostile packets that match a header will be rejected when the VPN software attempts to decrypt the header (col. 30, lines 53-67 and col. 30, lines 26-28).

Claim 9: Further, Munger teaches a small percentage of hostile packets that pass the fast packet filter will be rejected when matching pairs are not found in the active window or are active checkpoints (col. 30, lines 60-65).

Claim 10: Munger teaches communicating over the Internet using routers or servers using IP protocols to send normal-looking IP packet messages called TARP packets where the TARP packet contains a destination address (col. 7, lines 40-58), six nodes on an Ethernet and the network is to be split up into two private virtual networks with two sets of hardware addresses: one set for the VPN and a second set for the second VPN (col. 23, lines 11-20), regulating incoming packets by limiting the rate at which a transmitter can be synchronized with a receiver (col. 20, lines 6-10), and to identify the link key, and to identify the link key needed to decrypt the outer layer of encryption of a packet where a receiving routing terminal may identify the transmitting terminal by the sender field (col. 8, lines 1-15).

Claim 11: Further, Munger teaches incoming addresses can be used as indices into a long vector, making comparisons fast and as new addresses are generated the presence vector is updated to reflect the information (col. 30, lines 28-33).

Claim 12: Further, Munger teaches six nodes on an Ethernet and the virtual private network is to be split up into two private virtual networks with two sets of hardware addresses: one set for the VPN and a second set for the second VPN (col. 23, lines 11-20).

Claim 13: Further, Munger teaches the decomposed address portions must match all four shorter presence vectors before further processing is allowed (col. 30, lines 41-67).

Claim 14: Further, Munger teaches a small percentage of hostile packets that pass the fast packet filter will be rejected when matching pairs are not found in the active window or are active checkpoints (col. 30, lines 60-65).

Claim 15: Munger teaches an algorithm governs the sequential selection of IP-address pairs; one sender and one receiver IP address (col. 15, lines 27-31), the combination of the algorithm, seed, and IP address block will be called a hopblock where the send address and receive address of the IP header of each outgoing packet are filled with the send and receive IP addresses generated by the algorithm (col. 15, lines 27-35), a request is received by proxy server which checks its rules and determines that not VPN is needed (col. 39, lines 61-66), the gate keeper has a rule to make a VPN which is established between the client and the requested target where the gatekeeper would provide the address of the destination to the proxy (col. 39, lines 42-

52), and six nodes on an Ethernet and the network is to be split up into two private virtual networks with two sets of hardware addresses: one set for the VPN and a second set for the second VPN (col. 23, lines 11-20), and the proxy server would receive the client's request and forward it to gatekeeper. Gatekeeper would determine that no special VPN was needed, but that the client was not authorized to communicate with non-VPN members. The gatekeeper would reject the request, causing the proxy server to return an error message to the client. (col. 40, lines 4-13)

Claim 16: Further, Munger teaches the proxy server would receive the client's request and forward it to gatekeeper. Gatekeeper would determine that no special VPN was needed, but that the client was not authorized to communicate with non-VPN members. The gatekeeper would reject the request, causing the proxy server to return an error message to the client. (col. 40, lines 4-13)

Claim 17: Further, Munger teaches when matching pairs are not found in the active window or are active checkpoints that hostile packets are rejected. Hostile packets that match a header will be rejected when the software attempts to decrypt the header. (col. 30, lines 61-67 and col. 40, lines 1-3)

Claim 18: Further, Munger teaches access to secure site has been requested, the proxy determines whether the user has sufficient security privileges to access the site, proxy transmits a message to gatekeeper requesting that a virtual private network

Art Unit: 2132

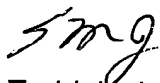
be created, the gatekeeper creates hopblocks to be used by the computer and secure target site for secure communication, the gatekeeper communicates these to user computer, proxy returns to user computer the resolved address passed to it by the gatekeeper using a secure administrative VPN. (col. 38, lines 23-42)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Todd M Jack whose telephone number is 703-305-1027. The examiner can normally be reached on M-Th, alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady, can be reached on 703-305-9595. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Todd Jack
Art unit 2133

July 6, 2004



Albert DeCady
Primary Examiner